



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/841,168	04/24/2001	John C. Droge	230074-0236	4113

7590 08/23/2005

Irvin C. Harrington, III
FOLEY & LARDNER
2029 Century Park East
Los Angeles, CA 90067-3000

EXAMINER

LEMMA, SAMSON B

ART UNIT	PAPER NUMBER
----------	--------------

2132

DATE MAILED: 08/23/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/841,168	Applicant(s) DROGE, JOHN C.	
	Examiner Samson B. Lemma	Art Unit 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 01 June 2005.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-55 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-55 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

[Handwritten mark]

DETAILED ACTION

1. This office action is in replay to an amendment filed on June 01, 2005. Claims

1, 14, 27, 36 and 42 have amended and **claims 1-55** are pending.

Response to Arguments

2. Applicant's remark/arguments filed on June 01, 2005 have been fully considered but they are not persuasive.

Applicants **amended** independent claims **1, 14, 27, 36 and 42** and added a new limitation in the above claims which was not part of the original claims. Applicants added the following limitation, "**non-packetized data**", Originally this added limitation was written as a simply "**data**".

Applicant first argument is based on the limitation in the independent claim 1.

Applicants made the following remark in support of the amendment, that Markandey, the reference on does not anticipate the features recited in claim 1.

First, Markandey does not teach or suggest "**encrypting the data a first time**" such that the data is once encrypted," as recited in claim 1. On page; 3, lines 7-8, the Action states that the claimed "encrypting data for a first time" is anticipated by the reference "DVD" of FIG. 7 from Markandey. In FIG. 7, Markandey discloses a transmitter that reads scrambled data from a DVD along with a Scramble-Pattern-11E) (see Markandey, paragraph [0075]), but

does not 15 disclose that the transmitter encrypts the data read from the DVD for a first time. Instead, the scrambled data of Markandey is stored on the DVD itself (see Markandey, paragraph [0075]). Thus, the transmitter does not perform scrambling. Since the transmitter of Markandey does not performing a step of scrambling data, it also does not include a step of "encrypting the data for a first time," and thus the transmitter does not anticipate this feature in claim 1. Therefore, Markandey does not anticipate claim 1.

Examiner disagrees with this argument. The examiner point out that the claim does not specify **the fact that the transmitter is the entity that performs the scrambling**, what is stated in the claim is the features of "encrypting the data a first time such that the data is once encrypted", this limitation indicates the fact that that some how the data is encrypted for the first time and as far as the reference on the record is concerned, Markandey, indeed disclosed this limitation [See figure 7, "Scrambled data"].

The specification is not the measure of invention. Therefore, limitations contained therein can not be read into the claims for the purpose of avoiding the prior art. See In re Sporck, 55 CCPA 743, 386 F. 2d 924, 155 USPQ 687 (1968)

The second argument made by the applicant is recited as follows,

Encryption and scrambling are different processes according to Markandey. On page 3, lines 7-8, the Action states the claimed step of "encrypting the data for a first time" is anticipated by the scrambled data in FIG. 7 of Markandey. However, in the description, Markandey distinguishes between encryption and scrambling. Specifically, Markandey describes the encryption process as encoding data using the Data Encryption Standard (DES), which encrypts 64-bit blocks of data using a 64-bit session key to produce a 64-bit encrypted result (see Markandey, paragraph [0025]). Thus, Markandey describes encryption

as a process of encoding data using a key. In contrast, Markandey describes scrambling as interchanging the order of various digital bits according to a scramble pattern, and provides examples of various scramble patterns in Table 5 (see Markandey, paragraph [0071]).

Clearly, Markandey does not consider encryption equivalent to scrambling. Thus, scrambling is not the same as or equivalent to encryption in the system of Markandey. Therefore, even if Markandey taught scrambling as a step in his process, this reference would not anticipate claim 1 since scrambling is not equivalent to encryption according to Markandey.

Examiner disagrees with this argument, as far as the Marandey is concerned the scrambling is done by interchanging the order of the various digital bits according to a scramble pattern such as shown below.[see paragraph "0071"]. The ultimate purpose of encryption process is to scramble a message so that the data is transformed into unreadable form by different techniques. Both processes, namely "Encryption" and "Scrambling" are used for deliberately concealing the data so that the data will be transmitted securely to it's intended destination. The **"19TH Updated, Improved and Expanded Edition, Newton's Telecom Dictionary, define the term, Encryption as "A fancy term for scrambling a message** so that no one can read it except the person for whom it's intended.

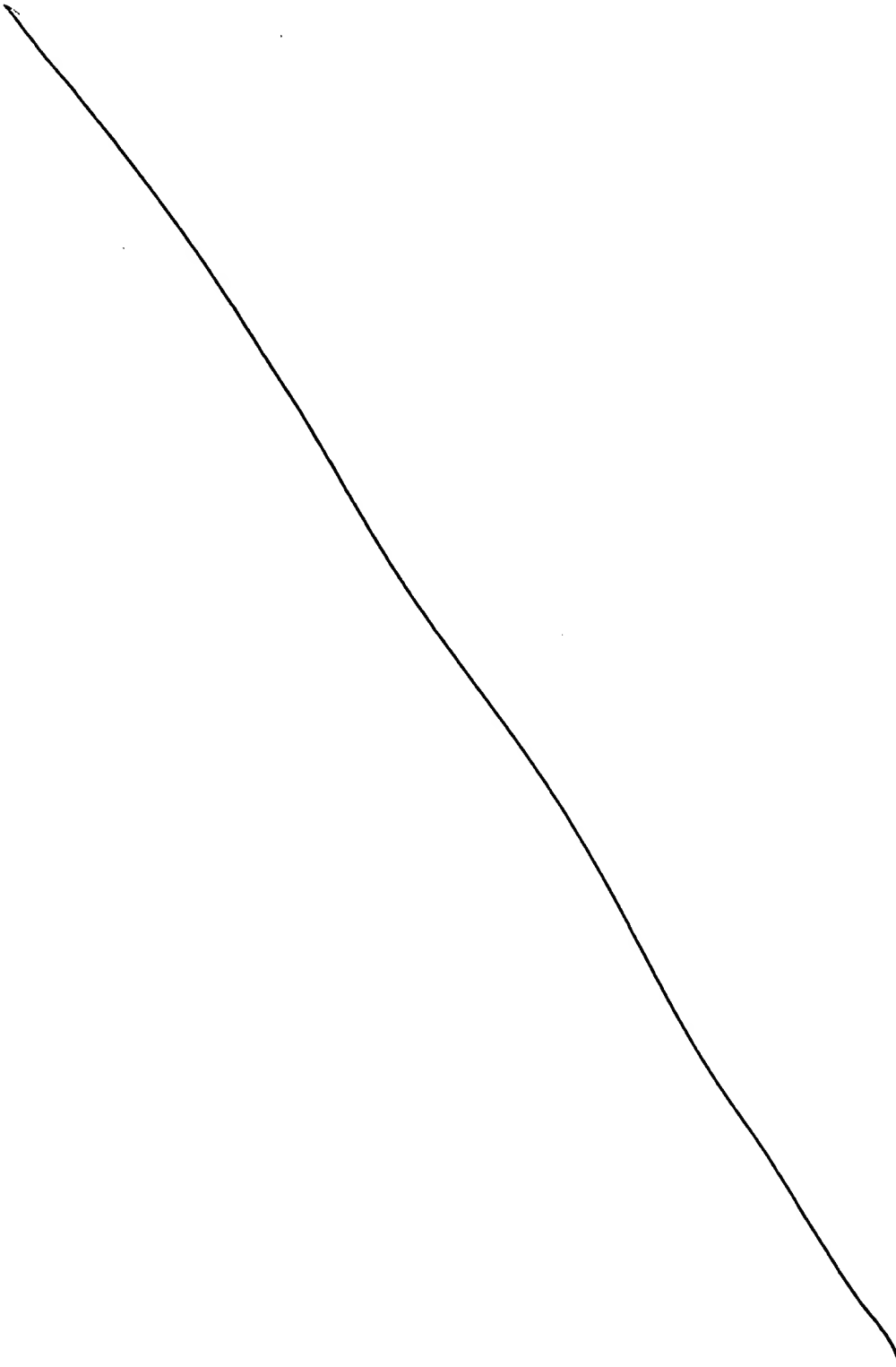
Both processes, "Encryption" and "Scrambling" are used for security purposes and they are not patentably distinguishable terms as long as they are used for the same purposes. These terms are usually used interchangeably to mean one and the same thing or perform one and the same function and this is clear for one of ordinary skill in the art.

Art Unit: 2132

"Encrypting a message" and "Scrambling a message" are for instance mean one and the same thing as far as the above dictionary's definition is taken into account.

The third argument by the applicant is in relation to the independent claim 14.

Applicant recited the following in support of his argument.

A large, hand-drawn diagonal line crossing the page from the upper left to the lower right, likely indicating a redaction or a placeholder for content.

receiving packetized, twice encrypted data; decrypting the packetized, twice encrypted data a first time such that the packetized data is once decrypted; reconstructing the non-packetized, once decrypted data; and decrypting the reconstructed, once decrypted data a second time." (emphasis added).

For at least the following two reasons, Markandey does not teach or suggest all of the features of claim 14.

First, Markandey does not teach or suggest "receiving packetized, twice encrypted data," as recited in claim 14. On page 3, line 16, the Action states that the receiver of Markandey in FIG. 7 anticipates the claimed step of "receiving packetized, twice encrypted data." **However, for reasons discussed above, Markandey does not disclose a transmitter that sends twice encrypted data. Instead, the data transmitted to the receiver in FIG. 7 of Markandey is only once encrypted** (see Markandey, paragraphs [0075]-[0076]). This means that the receiver of Markandey does not receive twice encrypted data. Thus, Markandey does not teach or suggest or suggest "receiving packetized, twice encrypted data," as recited in claim 14. Therefore, Markandey does not anticipate claim 14.

Second, Markandey does not teach or suggest "**reconstructing the non-packetized, once decrypted data; and decrypting** the reconstructed, once decrypted data a second time," as recited in claim 14 as amended. Markandey only discloses a single decryption and a single 17 descrambling (see Markandey, paragraphs [0075]-[0076]), but does not disclose a second decryption. As discussed above, Markandey distinguishes between scrambling and encryption, which implies that descrambling at the receiver in Markandey is not equivalent to decryption. Also, the only decryption discussed in Markandey is on data in IEEE 1394 packets (see Markandey, paragraph [0076]); however, Markandey does not disclose decryption of reconstructed, **non-packetized**, once decrypted data. Thus,

Examiner disagrees with this argument, since applicant's argument is mainly based on his argument presented for claim 1 and the examiner response provided to claim 1 is also applicable towards this argument.

Applicant 4th argument is regarding the independent claim 42 and is related to the motivation, Applicant recited the following in support of his argument.

The Action does not identify proper motivation for combining Markandey with Peirce, Jr. On page 9 lines 4-6, the Action states:

"It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to introduce two layers coordination and encryption techniques and using the internet as the method of communicating as per teaching of Peirce in to the method of as taught by Markandey, in order to avoid unnecessary duplication of encryption at different layers, ensure a more firmly security and provide secure services over the internet." Applicant respectfully disagrees. The motivation to combine stated in the Action only applies to the Peirce, Jr. reference, and is not relevant to the Markandey reference for at least the following two reasons. (1) The motivation suggested in the Action is motivation not to combine Markandey with Peirce, Jr. to render the claimed invention obvious. The Action states the motivation to combine is "to avoid **unnecessary** duplication of encryption at different layers" (emphasis added) on page 9. Since the Action interprets reading scrambled data from a DVD as encryption in Markandey (see at least page 8), the Action interprets Markandey as applying multiple encryptions to the scrambled data. However, the Action's interpretation of :Markandey as performing multiple encryptions would lead one of ordinary skill in the art not: to combine Markandey with a system that is designed to **avoid** a duplication of encryptions, such as that disclosed by Peirce, Jr. (see Peirce, Jr. col. 4, lines 13-55). The combination proposed in the Action would only have a single encryption in order to "avoid unnecessary duplication of encryption at different layers," and thus would not teach or suggest all of the features in claim

Art Unit: 2132

42, which requires a method that encrypts at both the Internet Protocol layer and at the data link layer (see claim 42, lines 2 and 4). Using the Action's reasoning of avoiding unnecessary duplication of encryption, Peirce, Jr. teaches away from being combined with the system of Markandey. Thus, one of ordinary skill in the art would not be motivated to combine Markandey with Peirce, Jr. because of the motivation from Peirce, Jr. not to combine, as stated in the Action. II) The motivation stated by the Action also provides further reasoning for not combining Markandey with Peirce, Jr. On page 9, the Action states that adding additional security to provide secure services for data transmission across the internet as motivation for combining Markandey with Peirce, Jr. However, securely transmitting services across the internet is irrelevant to the system of Markandey since the data transmitted in Markandey is across an IEEE 1394 bus, and not across the internet (see Markandey, paragraph [0003]). Although Markandey references TCP/IP networks in paragraph [0099], this reference does not state that the disclosed system transports data across the internet. Rather, Markandey states that the disclosed system "introduces to 1394. communication cryptographic techniques that have 24 been used in . . . TCP/IP networks." One of ordinary skill in the art would not be motivated to combine Markandey with Peirce, Jr. to "ensure a more firmly security and provide secure services over the internet" (emphasis added) since Markandey does not transmit data over the internet. Thus, there is no motivation to combine Markandey with Peirce, Jr., as suggested in the Action. Therefore, the Action does not establish a prima facie case of obviousness for combining Markandey with Peirce, Jr., and the rejection of claim 42 is improper.

Examiner disagrees with this argument, since applicant's primary argument is mainly based on his argument presented for claim 1 and the examiner response provided to claim 1 is also applicable towards this argument as to the argument made to the motivation, It is not necessary that the reference actually suggest, expressly or in so many words, the

Art Unit: 2132

changes or improvements that applicant has made. The text for combining references is what the references as a whole would have suggested to one of ordinary skill in the art. See *In re Sheckle*, 168 USPQ 716 (CCPA 1971) *In re McLaghin* 170 USPQ 209 (CCPA 1971). *In re Young* 159 USPQ 725 (CCPA 1968).

Applicant 5th argument is regarding the independent claim 50.

Applicant recited the following in support of his argument.

Claim 50 recites: "A method for receiving secure data comprising: receiving the data over a communication link; decrypting the data at a data link layer; and further decrypting the decrypted data at an Internet Protocol layer."

For reasons similar to those given for claim 44, the combination of Markandey with Peirce, Jr. does not teach or suggest "decrypting the data at a data link layer," and there is no motivation to combine Markandey with Peirce Jr. to render claim 50 obvious. Therefore, the Action does not establish a prima facie case of obviousness for combining Markandey with Peirce, Jr., and the rejection of claim 50 is improper.

Examiner disagrees with this argument, since applicant's primary argument is related to claim 44 and the examiner response provided to claim 44 is also applicable towards this argument as to the argument made to the motivation, It is not necessary that the reference actually suggest, expressly or in so many words, the changes or improvements that applicant has made. The text for combining references is what the references as a whole would have suggested to one of ordinary skill in the art. See *In re Sheckle*, 168 USPQ 716 (CCPA 1971) *In re McLaghin* 170 USPQ 209 (CCPA 1971). *In re Young* 159 USPQ 725 (CCPA 1968).

Applicant's other argument is regarding the dependent claims.

Applicants argued that the since the independent claims are patentable therefore all the claims dependent on the independent claims thereon are also in condition for allowance for the same reasons argued for the independent claims.

In response to the above argument by the applicant, the examiner response discussed to the independent claims presented above is also valid towards this argument.

Therefore all the **elements of the limitations of claim 1-55** is explicitly or implicitly or inherently suggested and disclosed by the reference/s on the records.

The rejections remains to be valid unless and otherwise the claims are further amended to introduce/include detail elements of the invention with out adding new matters and the claim limitation not the specification should contain limitation that are not taught/described/suggested/disclosed by the references on the record.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Art Unit: 2132

4. **Claim 1.4.11.14.17.19.27 and 36** is rejected under 35 U.S.C. 102(e) as being anticipated by Markandey et al. (hereinafter referred to as Markandey) (U.S. Publication No. 2002/0101989 A1).

5. **As per claim 1** Markandey discloses a method for securely transmitting data comprising:

- Obtaining non-packetized data on a computer system for transmission; (figure 7, reference "DVD")
- Encrypting the data a first time such that the data is once encrypted; (figure 7, reference "SCRAMBLED DATA" Shown at the "Transmitter")
- Packetizing the once encrypted data; (Figure 7, reference "1394 DATA PACKING")
- Encrypting the packetized, once encrypted data a second time such that the data is twice encrypted and transmitting the packetized, twice encrypted data. (Figure 7, reference "ENCRYPT")

6. **As per claim 14**, Markandey discloses a method for securely receiving data comprising:

- Receiving packetized, twice encrypted data; (Figure 7, reference "RECEIVER")
- Decrypting the packetized, twice encrypted data a first time such that the packetized data is once decrypted; (figure 7, reference "DECRYPT")
- Reconstructing the packetized, once decrypted data; (Figure 7, reference "1394 DATA UNPACK")

Art Unit: 2132

- Decrypting the reconstructed, once decrypted data a second time. (Figure 7, reference "DESCRAMBLE")

7. **As per claim 27 and 36, Kubota discloses** a method for securely transmitting and receiving data comprising:

- Obtaining non-packetized data on a first computer system for transmission; (Figure 7, reference "DVD")
- Encrypting the data a first time such that the data is once encrypted; (Figure 7, reference "SCRAMBLED DATA" shown at the "TRANSMITTER")
- Transmitting the once encrypted data from the first computer system to a first interface device; (Figure 7, reference "SCRAMBLED DATA" and "DIGITAL DATA LAYER" shown at the Transmitter) (As shown on figure 7, the "DVD" is first scrambled or encrypted and sent to the device or to the device shown on figure 7 as "DIGITAL DATA LAYER" on the transmitter side which is interpreted by the office as "the first interface device")
- Receiving the once encrypted data at the first interface device; (Figure 7, reference "DIGITAL DATA LAYER OF DPS") (the once encrypted or scrambled data is received at "the digital data layer" which is interpreted by the office as the first interface.)
- Packetizing the once encrypted data; (Figure 7, reference "1394 DATA PACKING")
- Encrypting the packetized, once encrypted data a second time such that the data is twice encrypted; (Figure 7, reference "ENCRYPT") and

Art Unit: 2132

- Transmitting the packetized, twice encrypted data from the first interface device to a second interface device; (Figure 7, reference “RECEIVER, “DIGITAL DATA LAYER OF DPS”) (The twice encrypted data is transmitted from the “Transmitter” in particular from the “first digital data layer” which is interpreted by the office as the “first interface” to the “RECIVER” in particular to the “DIGITAL DATA LAYER OF THE RECIVER” which is interpreted by the office as the second interface device)
- Receiving packetized, twice encrypted data at the second interface device; (Figure 7, reference “RECEIVER, “DIGITAL DATA LAYER OF DPS”) (The twice encrypted data is transmitted from the “Transmitter” in particular from the “first digital data layer” which is interpreted by the office as the “first interface” to the “RECIVER” in particular to the “DIGITAL DATA LAYER OF THE RECIVER” which is interpreted by the office as the second interface device)
- Decrypting the packetized, twice encrypted data a first time such that the packetized data is once decrypted (Figure 7, reference “DECRYPT”)
- Reconstructing the packetized, once decrypted data; (Figure 7, reference “1394 DATA UNPACK”)
- Transmitting the reconstructed, once decrypted data from the second interface device to a second computer system; (figure 7, reference “SCRAMBLED DATA” shown at the Receiver)
- Receiving the reconstructed, once decrypted data at the second computer system; (figure 2, ref. Num “17”) and decrypting the reconstructed, once decrypted data a second time. (Figure 7, reference “DESCRAMBLE”)

8. **As per claims 4**, **Markandey** discloses the method for securely transmitting data as applied to claim 1 above. Furthermore **Markandey** discloses the method wherein transmitting the once encrypted data from the computer system to an interface device; and receiving the once encrypted data at the interface device. (figure 7, reference "Transmitter, "DIGITAL DATA LAYER") (As explained above and shown on figure 7, reference "Transmitter, "DIGITAL DATA LAYER" is interpreted by the office as the 1st interface device and receives the once encrypted data or scrambled data as shown on figure 7.)
9. **As per claim 11**, **Markandey** discloses the method for securely transmitting data as applied to claim 1 above. Furthermore **Markandey** discloses the method wherein transmitting the packetized, twice encrypted data comprises transmitting the packetized, twice encrypted data from the interface device. (Figure 7, reference "RECEIVER, "DIGITAL DATA LAYER OF DPS") (The twice encrypted data is transmitted from the "Transmitter" in particular from the "first digital data layer" which is interpreted by the office as the "first interface" to the "RECEIVER" in particular to the "DIGITAL DATA LAYER OF THE RECIVER" which is interpreted by the office as the second interface device)
10. **As per claim 17**, **Markandey** discloses the method for securely transmitting data as applied to claim 14 above. Furthermore **Markandey** discloses the method wherein receiving packetized, twice encrypted data comprises receiving packetized, twice encrypted data at an interface device. (Figure 7, reference "RECEIVER, "DIGITAL DATA LAYER OF DPS") (The twice encrypted data is transmitted from the "Transmitter" in particular from the "first digital data layer" which is interpreted by the office as the "first

Art Unit: 2132

interface" to the "RECIVER" in particular to the "DIGITAL DATA LAYER OF THE RECIVER" which is interpreted by the office as the second interface device)

11. **As per claims 19**, Markandey discloses the method for securely transmitting data as applied to claim 17 above. Furthermore Markandey discloses the method wherein transmitting the reconstructed, once decrypted data from the interface device; and receiving the reconstructed, once decrypted data at a computer system. (figure 7, reference "SCRAMBLED DATA" at the Receiver)

Claim Rejections - 35 USC § 103

12. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

13. **Claims 2-3, 10, 12-13, 15-16, 18, 24, 26, 28-35, 37-45, 47-51, 53-55** are rejected under 35 U.S.C. 103(a) as being unpatentable over Markandey et al. (hereinafter referred to as Markandey) (U.S. Publication No. 2002/0101989 A1) in view of Peirce, Jr. et al. (hereinafter referred to as Peirce) (U.S. Patent No. 6,542,992)

14. **As per claim 42 and 44**, Markandey discloses

- Encrypting the non-packetized data (Figure 7, reference "SCRAMBLED DATA" shown at "Transmitter");

Art Unit: 2132

- Packetizing the data; (figure 7, reference "TRANSMITTER", 1394 DATA PACKING")
- Encrypting the packetized data (Figure 7, reference "ENCRYPT"); and
- Transmitting the packetized, encrypted data from one interface to the other. (figure 7).

Furthermore Markandey introduces the cryptographic techniques which is explained to be used in other communication environment such as cable modems, IP networks, smart cards and others.(Column 8, reference [0099])

Markandey does not explicitly disclose

- Encrypting the data at a data link layer; then encrypting the data at an Internet Protocol layer;

Transmitting the packetized, encrypted data from one interface to the other using network.

However, in the same field of endeavor, **Peirce** discloses

The method of coordination of encryption and compression for data en route from the host computer to the mobile station between different layers one of which is capable of performing PPP level encryption which is data link layer encryption as explained on the same reference on column 5, lines 27-29) and the other of which is capable of performing IP level or layer encryption.(Column 4, lines 46-52)

Peirce further discloses how the internet is used for communicating two interfaces (figure 2, ref. Num "20")

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to introduce two layers coordination and encryption

techniques and using the internet as the method of communicating as per teaching of **Peirce** in to the method of as taught by **Markandey**, in order to avoid unnecessary duplication of encryption at different layers , ensure a more firmly security and provide secure services over the internet.

15. **As per claim 50,** Markandey discloses a method for receiving secure data comprising:

- Receiving the data over a communication link; (Figure 7, reference "RECEIVER")
- Decrypting the packetized, twice encrypted data a first time such that the packetized data is once decrypted; (figure 7, reference "DECRYPT")
- Decrypting the reconstructed, once decrypted data a second time. (Figure 7, reference "DESCRAMBLE")

Markandey does not explicitly disclose

- Decrypting/encrypting the data at a data link layer; and further
- Decrypting/encrypting the decrypted data at an Internet Protocol layer.

However, in the same field of endeavor, **Peirce** discloses

The method of coordination of encryption/decryption for data en route from the host computer to the mobile station between different layers one of which is capable of performing PPP level encryption/decryption which is data link layer encryption as explained on the same reference on column 5, lines 27-29 and the other of which is capable of performing IP lever encryption/decryption.(Column 4, lines 46-52)

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to introduce two layers coordination and decryption/encryption techniques as per teachings of **Peirce** in to the method as taught by Markandey, in

order to avoid unnecessary duplication of encryption/decryption at different layers and to ensure a more firmly security.

16. **As per Claims 2, 3, 28, 29, 37 and 38 Markandey** discloses the method of

- Encrypting the data a first time such that the data is once encrypted; (figure 7, reference "SCRAMBLED DATA" shown at the "Transmitter")
- Encrypting the packetized, once encrypted data a second time such that the data is twice encrypted; (Figure 7, reference "ENCRYPT")

Markandey does not explicitly disclose

Encrypting the data a first time comprises encrypting the data at a data link layer and encrypting the packetized, once encrypted data a second time comprises encrypting the data at an Internet Protocol layer.

However, in the same field of endeavor, **Peirce** discloses

The method of coordination of encryption and compression for data en route from the host computer to the mobile station between different layers one of which is capable of performing PPP level encryption which is data link layer encryption as explained on the same reference on column 5, lines 27-29 and the other of which is capable of performing IP level/layer encryption. (Column 4, lines 46-52)

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to introduce two layers coordination and encryption techniques as per teaching of **Peirce** in to the method of as taught by **Markandey**, in order to avoid unnecessary duplication of encryption at different layers and to ensure a more firmly security.

17. **As per claim 18, 34 and 39**, Markandey discloses the method of decrypting the packetized, twice encrypted data a first time such that the packetized data is once decrypted (Figure 7, reference "DECRYPT")

Markandey does not explicitly disclose decrypting the packetized, twice encrypted data a first time comprises decrypting the packetized, twice encrypted at an Internet Protocol layer.

However, in the same field of endeavor, **Peirce** discloses the method of coordination of encryption/decryption and compression/decompression for data en route from the host computer to the mobile station between different layers one of which is capable of performing PPP level /layer encryption/decryption which is data link layer encryption/decryption as explained on the same reference on column 5, lines 27-29, and the other of which is capable of performing IP lever encryption/decryption.(Column 4, lines 46-52)

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to introduce two layers coordination and encryption/decryption techniques as per teaching of **Peirce** in to the method of as taught by **Markandey**, in order to avoid unnecessary duplication of encryption/decryption at different layers and to ensure a more firmly security.

18. **As per claims 24, 35 and 40** Markandey discloses the method of Receiving the reconstructed, once decrypted data at the second computer system; (figure 2, ref. Num "17") and decrypting the reconstructed, once decrypted data a second time. (Figure 7, reference "DESCRAMBLE"). **Markandey** does not explicitly disclose decrypting the reconstructed, once decrypted data a second time comprises decrypting the reconstructed, once decrypted data at a data link layer.

However, in the same field of endeavor, **Peirce** discloses the method of coordination of encryption/decryption and compression/decompression for data en route from the host computer to the mobile station between different layers one of which is capable of performing PPP level encryption/decryption which is data link layer encryption/decryption as explained on the same reference on column 5, lines 27-29.(Column 4, lines 46-52)

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to introduce two layers coordination and encryption/decryption techniques as per teaching of **Peirce** in to the method of as taught by **Markandey**, in order to avoid unnecessary duplication of encryption/decryption at different layers and to ensure a more firmly security.

19. **As per claims 12,13,15,16, 30-33, 41, 43, 48,49,54 and 55**, Markandey discloses the method of transmitting data using cable modem, TCP /IP network, Internet privacy-Enhanced Mail (PEM), Smart Cards and defence applications (Page 8, reference "[0099]")

Furthermore Markandey discloses

Transmitting the packetized, twice encrypted data from the first interface device to a second interface device; (Figure 7, reference "RECEIVER, "DIGITAL DATA LAYER OF DPS") (The twice encrypted data is transmitted from the "Transmitter" in particular from the "first digital data layer" which is interpreted by the office as the "first interface" to the "RECEIVER" in particular to the "DIGITAL DATA LAYER OF THE RECEIVER" which is interpreted by the office as the second interface device)

Art Unit: 2132

Markandey does not explicitly disclose transmitting the packetized, twice encrypted data comprises transmitting the packetized, twice encrypted data over a network or internet.

However, in the same field of endeavor, **Peirce** discloses the method of communicating two interfaces using internet.(figure 1, ref. Num "20")

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to create a communication between two interfaces through network/internet as per teachings of **Peirce** in to the method of as taught by **Markandey**, for the function of having a capability to provide services with security over the internet.

20. **As per claims 10, 26, 47 and 53,** the combinations of **Markandey** and **Peirce** discloses the method for securely transmitting data as applied to claims 3, 18, 44 and 50. Furthermore **Peirce** discloses the method wherein data encrypted at an Internet Protocol layer is encrypted using Internet Protocol Security protocols.(Column 4, lines 51-52) (IPSec offers security at the Network layer and the encryption is made to provide security at the network layer and this meets the recitation of the limitation)
21. **As per claims 45** the combinations of **Markandey** and **Peirce** discloses the method for securely transmitting data as applied to claim 44. Furthermore **Markandey** discloses the method comprising the step of packetizing the data. (Figure 7, reference "1394 DATA PACKING")
22. **As per claims 51,** the combinations of **Markandey** and **Peirce** discloses the method for securely transmitting data as applied to claim 50. Furthermore **Markandey** discloses the

Art Unit: 2132

method further comprising the step of reconstructing the data. (Figure 7, reference "1394 DATA UNPACK")

23. **Claims 5-8 and 20-23** are rejected under 35 U.S.C. 103(a) as being unpatentable over Markandey et al. (hereinafter referred to as **Markandey**) (U.S. Publication No. 2002/0101989 A1) in view of **Blom**, Martin. (hereinafter referred to as **Blom**) (European Publication, Publication Number EP 0406187 A1)

24. **As per claims 5 and 6**, **Markandey** discloses the method of transmitting data using the modem.(Page 8, reference "[0099]")

Markandey further discloses transmitting the once encrypted data from the first computer system to a first interface device; (Figure 7, reference "SCRAMBLED DATA" and "DIGITAL DATA") (As shown on figure 7, the "DVD" is first scrambled or encrypted and sent to the device or to the device shown on figure 7 as "DIGITAL DATA LAYER" on the transmitter side which is interpreted by the office as "the first interface device")

Markandey does not explicitly disclose

Transmitting the once encrypted data comprises transmitting the once encrypted data using a modem and the modem is an encrypting modem.

However, in the same field of endeavor, **Blom** discloses modem which has encrypting equipment installed in it, encrypting data and transmitting the data to the telecommunication network. (Column 1, lines 11-25)

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to introduce encryption using modem as per teaching of **Blom** in to the method of as taught by **Markandey**, in order to prevent unauthorized tapping of data as data are transmitting through the telecommunication network.

25. **As per claims 7 and 8, Markandey** discloses the method of transmitting data using the modem.(Page 8, reference “[0099]”)

Markandey further discloses receiving the once encrypted data at the first interface device; (Figure 7, reference “DIGITAL DATA LAYER OF DPS”) (the once encrypted or scrambled data is received at “the digital data layer” which is interpreted by the office as the first interface.)

Markandey does not explicitly disclose

The method of receiving the once encrypted data comprises receiving the once encrypted data using a modem and the modem is an encrypting modem.

However, in the same field of endeavor, **Blom** discloses modem which has encrypting equipment installed in it, encrypting data and transmitting/receiving data to/from the telecommunication network. (Column 1, lines 11-25; figure 1)

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to introduce encryption using modem as per teachings of **Blom** in to the method of as taught by **Markandey**, in order to prevent unauthorized tapping of data as data are transmitting from the first interface to the second interface.

26. **As per claims 20 -23, Markandey** discloses the method of transmitting data using the modem.(Page 8, reference “[0099]”)

Markandey further discloses

- Decrypting the packetized, twice encrypted data a first time such that the packetized data is once decrypted (Figure 7, reference “DECRYPT”)

Art Unit: 2132

- Reconstructing the packetized, once decrypted data; (Figure 7, reference “1394 DATA UNPACK”)
- Transmitting the reconstructed, once decrypted data from the second interface device to a second computer system; (figure 7, reference “DESCRAMBLED DATA” shown at the “Receiver”)

Markandey does not explicitly disclose transmitting the reconstructed, once decrypted data comprises transmitting the reconstructed, once decrypted data using a decrypting modem and receiving the reconstructed, once decrypted data using a decrypting modem.

However, in the same field of endeavor, **Blom** discloses modem which has encrypting equipment and decrypting equipment installed in it, encrypting or decrypting data and transmitting/receiving data to/from communicating devices. (Column 1, lines 11-25; figure 1; column 1, lines 55-column 2, line 2)

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to introduce encryption/decryption using modem as per teaching of **Blom** in to the method of as taught by **Markandey**, in order to prevent unauthorized tapping of data as data are transmitting from the first interface to the second interface and from the second interface to the receiving device.

27. **Claim 9 and 25** is rejected under 35 U.S.C. 103(a) as being unpatentable over **Markandey** et al. (hereinafter referred to as Markandey) (U.S. Publication No. 2002/0101989 A1) in view of **Moberg** et al. (hereinafter referred to as **Moberg**) (U.S. Patent No 6,697,872)

28. **As per claim 9, Markandey discloses** transmitting the packetized, twice encrypted data from the first interface device to a second interface device; (Figure 7, reference "RECEIVER, "DIGITAL DATA LAYER OF DPS") (The twice encrypted data is transmitted from the "Transmitter" in particular from the "first digital data layer" which is interpreted by the office as the "first interface" to the "RECIVER" in particular to the "DIGITAL DATA LAYER OF THE RECIVER" which is interpreted by the office as the second interface device)

Markandey does not explicitly disclose transmitting the packetized, twice encrypted data comprises transmitting the packetized, twice encrypted data using a network interface card.

However, in the same field of endeavor, **Moberg** discloses using network interface card when the system includes a source and destination nodes (end systems)(column 1, lines 37-40). **Moberg** further discloses how line cards control the sending and receiving of data packets over the network.(Column 4, lines 43-45)

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to introduce network interface card as per teachings of **Moberg** in to the method of as taught by Markandey, for the purpose of using any device with the interface cards for communicating source and destination nodes.

29. **Claims 46 and 52** are rejected under 35 U.S.C. 103(a) as being unpatentable over Markandey et al. (hereinafter referred to as **Markandey**) (U.S. Publication No. 2002/0101989 A1) in view of Peirce Jr. et al. (hereinafter referred to as **Peirce**) (U.S. Patent No. 6,542,992) further in view of Moberg et al. (hereinafter referred to as **Moberg**) (U.S. Patent No 6,697,872)

30. **As per claims 46 and 52**, the combination of **Markandey** and **Peirce** discloses the method of transmitting and receiving data as explained on claims 44 and 50 above. Furthermore **Markandey** discloses

Art Unit: 2132

- Transmitting the once encrypted data from the first computer system to a first interface device; (Figure 7, reference “SCRAMBLED DATA” and “DIGITAL DATA LAYER” shown at the Transmitter) (As shown on figure 7, the “DVD” is first scrambled or encrypted and sent to the device or to the device shown on figure 7 as “DIGITAL DATA LAYER” on the transmitter side which is interpreted by the office as “the first interface device”)
- Receiving the once encrypted data at the first interface device; (Figure 7, reference “DIGITAL DATA LAYER OF DPS” at the transmitter) (the once encrypted or scrambled data is received at “the digital data layer” which is interpreted by the office as the first interface.)

The combination of **Markandey** and **Peirce** does not explicitly disclose transmitting the data comprises transmitting the data using a network interface card.

However, in the same field of endeavor, **Moberg** discloses using network interface card when the system includes a source and destination nodes (end systems)(column 1, lines 37-40). **Moberg** further discloses how line cards control the sending and receiving of data packets over the network.(Column 4, lines 43-45)

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to introduce network interface card as per teaching of **Moberg** in to the method of as taught by the combination of **Markandey** and **Peirce**, for the purpose of using any device with the interface cards for creating a secure communication link between the source and destination nodes.

Conclusion

Art Unit: 2132

31. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

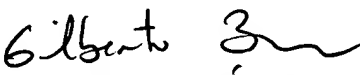
A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm). If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SAMSON LEMMA

S.L.
08/18/2005


GILBERTO BARRÓN JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100